IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	**GATTO, Jean-Marie et al.**	Exr:	**Nirav B. PATEL**
Serial Number:	**10/789,975**	Art Unit:	**2135**
Filed	**February 27, 2004**	Confirm No.:	**9438**
For:	**Dynamic Configuration of a Gaming System**	Cust. No.:	**86915**
Att'y Dckt No.:	**CYBS5858**		**PRE-APPEAL BRIEF REQUEST FOR RECONSIDERATION**

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The present Pre-Appeal Brief Request for Review is submitted subsequent to the Request for Reconsideration of March 22, 2010 and in response to the Final Office Action November 24, 2009. This Request is filed with the fee for a two-month extension of time, Large Entity.

I. Claim 25 has yet to be substantively examined.

Despite respectfully requesting for a substantive examination of claim 17 several times previously, the Office again dismissed (see Advisory Action of 04/06/2010) claim 25 as encompassing *"limitations that are similar to claim 17. The claim limitation "packaging the code singed [sic] authorized software component into an installation package" is nothing more than just executable software with signature."*

Claim 25, however, recites:

> **packaging the code signed authorized software components into an installation package;**
>
> **configuring install policies to install each code signed authorized executable software component contained in the installation package;**
>
> **configuring certificate rule policies to allow execution of the installed code signed authorized executable software component;**
>
> **configuring enforcement of the policies.**

Not once has the Office discussed the steps of "**configuring install policies**...; **configuring certificate rule policies**...; **configuring enforcement of the policies**" or applied any art thereto. These positively recited steps are <u>not</u> found in claim 17 or in any of the other independent claims. As such, they merit a considered substantive examination (what the applicant paid for) and not an out-of-hand dismissal that they are "similar to" the packaging steps of other claims when these steps, in fact, have no counterparts in any of the other pending claims. Moreover, the Office Review panel is also urged to consider the arguments beginning in the middle of page 13 of the Request for Reconsideration of March 22, 2010, relative to the "KSR" case. The lack of substantive examination of claim 25 alone, it is respectfully submitted, warrants withdrawal of the finality of the outstanding Office Action and the issuance of either a <u>new non-final Office Action</u>, or a Notice of Allowance, as appropriate.

II. The Office's Interpretation of Gunyakti et al. is Factually Incorrect

Claim 17 recites "producing a separate and unique PKI certificate for each of the plurality of executable software components subject to receiving certification within each gaming machine, each software component

subject to receiving certification including a unique identifier; code signing each executable software component subject to receiving certification with its respective separate and unique PKI certificate"

Gunyakti et al. does not teach generating a **separate and unique** PKI certificate **for each executable software component**, nor does Gunyakti use generated PKI certificates to code sign each of the different executable software components within each gaming machine. Instead, Gunyakti et al. generates a **volume license** for a number of products and it is this volume license that is signed with a private key to generate the license file 224 – see paragraph [0027]. Therefore, it is the volume license itself that is signed with a private key and NOT "each of the plurality of executable software components", as required and claimed. In the Advisory Action, the Examiner states "*Therefore, each unique software associated with unique enterprise specific VLK for a plurality of users*". However, the claims do not recite that each software is associated with a unique volume license – for one or a plurality of users. The claims simply require "a separate and unique PKI certificate for each ... executable software component" and "code signing each executable software component ... with its respective separate and unique PKI certificate.". As claimed, **each executable software components is code signed with its associated "separate and unique" PKI certificate**. In direct contrast, in Gunyakti, it is the license to use the software that is signed, and not the software components themselves, as in the claimed embodiments. This factual error represents yet another independent ground for allowing this application or re-opening the prosecution thereof, as appropriate.

III.   The Office's Interpretation of Yip et al. is Also Factually Incorrect

The Office relies upon **Yip** for the same teaching of producing a separate and unique PKI certificate for each of the plurality of executable software components subject to receiving certification within each gaming machine, and points to Figs. 2 and 3 and paragraphs 0048 and 0046.

In Yip, a conventional Certificate Authority (CA) issues a certificate 106 and an application-specific CA issues a corresponding application-specific certificate 206. See paragraph 0042. The certificate 106 and application certificate 206 are linked, such that when the certificate 106 is revoked, the application-specific certificates are also preferably revoked. See paragraph 0044. Thus, the application-specific certificate 206 is a "companion" to the certificate 106.

Note, however, that claim 17 recites:

> **code signing each executable software component subject to receiving certification with its respective separate and unique PKI certificate, each respective PKI certificate being uniquely identified at least by a unique identifier that is uniquely associated with the executable software component such that identical executable software components in different ones of the plurality of gaming machines of the network connected gaming system are associated with identical identifiers and are code signed with identical PKI certificates, such that non-identical executable software components in different ones of the plurality of gaming machines are associated with separate and different identifiers and are code signed with separate and different PKI certificates and such that no two non-identical executable software components in different gaming machines are code signed with a same PKI certificate,** (underlining for emphasis)

As the application-specific certificate 204 is "for use with the **particular application 201**", it **necessarily follows** that identical executable software components in different ones of the plurality of gaming machines, in

Yip, would be associated with different PKI certificates, as each application (each "**particular application 201**", in Yip's language) would receive a different certificate 106 and corresponding different application-specific certificates 206. There is no teaching or suggestion in Yip otherwise.

Indeed, Yip teaches away from the claimed embodiments in which **identical application-specific certificates** are provided for identical executable software components in different machines. In other words, the CA in Yip would not issue identical certificates 106 to more than one machine/user nor would the CA issue identical companion application-specific certificates 206 to more than on machine/user, as each certificate 106 is different and as the application-specific certificates 206 are companions to such different certificates 106.

Therefore, since each "particular" application 201 receives a different certificate in Yip, there are believed to be no grounds for holding that Yip teaches or suggests (either alone or in combination with any or all of the other three applied references), the claimed limitation:

> **identical executable software components in different ones of the plurality of gaming machines of the network connected gaming system are associated with identical identifiers and are code signed with identical PKI certificates**

Therefore, the combination of Gunyakti and Yip does not yield the claim limitation (contrary to that stated in the advisory action of 4/6/10, beginning at line 7), but instead would teach a PKI signed volume license (Gunyakti) in combination with application-specific certificates in which each application received its own certificate, with identical executable software components on different gaming machines receiving different application-specific certificates 204, as again taught by Gunyakti, which combination suggests nothing of the claimed embodiments and teaches away from any embodiment in which "identical executable software components in different ones of the plurality of gaming machines of the network connected gaming system are associated with identical identifiers and are code signed with identical PKI certificates", as claimed herein.

IV. Fieres Does not Remedy The Fundamental Shortcomings of Gunyakti-Yip

The applied reference to **Fieres** teaches the issuance of application certifications to insure that applications operate at the proper cryptographic level granted for that application by an application domain authority 22. However, there is no teaching or suggestion in Fieres that "identical executable software components in different ones of the plurality of gaming machines of the network connected gaming system are associated with identical identifiers and are code signed with identical PKI certificates". Nor is there any teaching or suggestion in Fieres that "non-identical executable software components in different ones of the plurality of gaming machines are associated with separate and different identifiers and are code signed with separate and different PKI certificates", as claimed herein.

Fieres does not teach or suggest that "no two non-identical executable software components in different gaming machines are code signed with a same PKI certificate", as claimed herein -- nor has the Office identified where such teachings or suggestions may be found. In fact, there is no teaching or suggestion, in the context of the distribution of cryptographic capabilities, that Fieres would allow identical executable components in different

machines to have identical certificates, as required herein. Such would surely defeat the security measures. A general allegation that Fieres teaches application certificates with application IDs (see Advisory Action) does not, without more, rise to the level of teaching the aforementioned claim limitations, whether considered singly or in combination with the other applied references.

V. Lambert Also Does not Provide the Missing Teachings or Suggestions

Lastly, **Lambert** was relied on for a teaching of *"a method and system for securely control software execution by identifying and classifying software and locating a rule and associated security level for executing executable software"* (Advisory action of 4/6/2010). However, the pending claims do not **a)** identify software, **b)** classify software, **c)** locate a rule and/or **d)** locate an associated security level. More to the point, with respect to what **is actually** claimed, Lambert does not teach a software restriction policy certificate rule for each executable software component. Quite to the contrary, Lambert teaches **one rule for an entire security level** for executing executable software (see Abstract, lines 3-4). This means that executable software, in Lambert et al. are associated with different security levels, and the rule for that security level may allow or disallow execution thereof. Lambert also teaches a hierarchy of rules, to help distinguish which rule to use, should a piece of software have multiple classifications (see Abstract, last sentence). In Column 15, lines 29-36, Lambert teaches how rules are selected and at lines 15-20 describes how rules determine the execution of the file. In Lambert, therefore, there is demonstrably no one-to-one relationship (a SRP for each executable software components) with executable software components and rules, as required by claim 17:

> **configuring a software restriction policy certificate rule for each of the plurality of executable software components and enforcing each of the software restriction policy certificate rules to allow execution of only those executable software components whose code signed PKI certificate is determined to be authorized.**

To the contrary, Lambert et al. teaches away from the claimed embodiments by teaching a one-to-many relationship between the security rules and the executable software components, which is antithetical to the claimed embodiments, which require a software restriction policy for EACH of the plurality of executable software components. The applied combination, therefore, cannot be said to teach or to suggest the embodiment defined by claim 17.

The arguments presented above relative to claim 17 are equally applicable to claim 20. Rather than repeat these here, reference is made to the arguments above, incorporated herein in their entirety.

Claim 22, rejected as being unpatentable over Lambert-Gunyakti-Yip, includes a code signing step that is similar to that of claim claims 17 and 20, and the above arguments relative to Gunyakti and Yip apply. Although Lambert does teach rules based upon a path in Column 13, the applied combination of Lambert-Gunyakti-Yip does not teach or suggest the claimed software restriction policy configuring and code signing steps, nor, by extension, the claimed step of:

> **enforcing the certificate software restriction policy configured for each of the code signed authorized executable software components of each of the constituent computers of**

the gaming system, and

for the same arguments presented relative to claim 17, which are also incorporated herein in their entirety.

Claim 24 recites the step of "producing a separate and unique PKI certificate for each of the plurality of executable software components within the gaming system subject to receive certification", and is believed to be allowable over the applied combination for the reasons developed above. Moreover, claim 24 also recites:
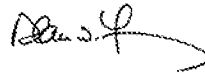
> **code signing each software component subject to receive certification with its respective separate and unique PKI certificate;**
>
> **configuring a certificate software restriction policy for each of the respective separate and unique PKI certificates, and**
>
> **enforcing the certificate software restriction policy for each of the respective separate and unique PKI certificates.**

In contradistinction, the primary reference to Gunyakti advocates volume licenses (➔ how can a **volume** license be interpreted as a "separate and unique PKI certificate for each of the plurality of executable software components"?), Yip advocates companion application-specific certificates and Lambert calls for a hierarchy of rules to enable the application of a specific rule to a specific application. The applied combination does not teach code signing <u>each</u> software component subject to receive certification with its respective separate and unique PKI certificate (compare to Gunyakti's volume licenses), configuring a certificate software restriction policy for each of the respective separate and unique PKI certificates (compare with the one-to-many relationship of Lambert's rules to the applications) or enforcing the certificate software restriction policy for each of the respective separate and unique PKI certificates, as claimed herein.

None of the applied references, alone or in combination, teach or suggest the claimed embodiments. The prior art (Yip) teaches that each "particular" software is signed with a different certificate. The prior art (Gunyakti) also teaches code signing volume <u>licenses</u> (≠ executable <u>software components</u>). The prior art also teaches security levels (Lambert) or cryptographic levels and rules (Fieres) that may or may not allow execution of software components. It is respectfully submitted that the claimed elements are most assuredly <u>not</u> combined "*according to known methods*", as the Office asserts -- nor would <u>any</u> combination of these references teach, suggest or result in the claimed embodiments. Therefore, reconsideration and withdrawal of the obviousness rejections are respectfully requested.

Respectfully submitted,

Date: _____April 24, 2010_____   By: _____
                  Alan W. Young
                  Attorney for Applicants
                  Registration No. 37,970

YOUNG LAW FIRM, P.C.
4370 Alpine Rd., Ste. 106
Portola Valley, CA 94028
Tel.: (650) 851-7210
Fax: (650) 851-7232 C:\YLF\CLIENTS\CYBS\5858 (Trusted Game Download)\5858 Pre-Appeal Brief Req For Recon of 04-24-2010.doc

Doc Code: AP.PRE.REQ

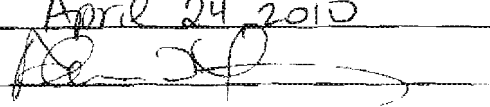| PRE-APPEAL BRIEF REQUEST FOR REVIEW	Docket Number (Optional)
	CYBS5858

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]	Application Number	Filed
on _April 24, 2010_	10/789,975	Feb 27, 2004
Signature	First Named Inventor	
	GATTO, Jean-Marie	
Typed or printed name Alan W. Young	Art Unit	Examiner
	2135	Nirav B. Patel

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
       Note: No more than five (5) pages may be provided.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

☑ attorney or agent of record. 37,970
Registration number

☐ attorney or agent acting under 37 CFR 1.34.

Registration number if acting under 37 CFR 1.34 _____

_____ Signature

Alan W. Young
Typed or printed name

650-851-7210
Telephone number

April 24, 2010
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required.
Submit multiple forms if more than one signature is required, see below*.

☑ *Total of __1__ forms are submitted.